Public Key Infrastructure Roadmap for the Department of Defense

29 October 1999

Version 3.0

Prepared By:

DoD Public Key Infrastructure Program Management Office

Approved:

_____

Assistant Secretary of Defense

(Command, Control, Communications, and Intelligence)

Table of Contents

Table of Contents		i
Figures		v
Executive Summary		1
1.	Introduction	1
1.1	Public Key Enabled System Elements	1
1.1.1	Certificate Management	2
1.1.2	Registration	3
1.1.3	Applications	3
1.1.4	Defense in Depth	4
2.	Target DoD PKI	5
2.1	Target Objectives	5
2.2	Target Architecture Overview	6
2.2.1	Target Certificate Management	7
2.2.2	Target Registration Concept	10
3.	Strategy to Achieve Target	13
4.	Issues	19
4.1	Transition Issues	19
4.1.1	Funding	19
4.1.2	Architecture Extensions	19
4.2	Technical Risks	20

4.2.1 Application Processing 20
4.2.2 Revocation Architecture 20
4.2.3 Privilege 20
4.2.4 Interoperability 21
4.2.5 Scalability 21
4.2.6 Directories 22
4.3 Tactical Concerns 22
5. Roles and Responsibilities 23
5.1 Program Management 23
5.2 Requirements 23
5.2.1 Security 23
5.2.2 Functional and Operational 23
5.3 Interoperability 23
5.4 Development 23
5.5 Procurement 24
5.5.1 DoD PKI Program Management Office (PMO) 24
5.5.2 Services, and Agencies 24
5.6 Operations 24
5.6.1 Root CA(s) 24
5.6.2 CA Servers and Central Directories 24
5.6.3 RAs and Local Directories 25
5.6.4 Help Desk 25
5.7 Oversight 25
Appendix A. Policy Management 1

Appendix B. DoD PKI Requests 4

Appendix C. Definitions 1

Appendix D. PKI Milestones 1

References 1

Abbreviations and Acronyms 3

Figures

Figure 1.	Public Key Enabled System	2
Figure 2.	Target DoD PKI Architecture	7
Figure 3.	Target User Registration Process	11
Figure 4.	Schedule	17
Figure 5.	DoD Certificate Management Process	A-1

Executive Summary

The Department of Defense (DoD) Key Management Infrastructure (KMI) is the critical underpinning of the Department's Information Assurance (IA) capabilities and is a vital element in achieving a secure IA posture for the Defense Information Infrastructure (DII). Accordingly, it is imperative that the Department takes an aggressive approach in acquiring a KMI that meets the requirements for all IA services. The DoD Public Key Infrastructure (PKI) is an essential element and a major component of the KMI.

PKI, as defined herein, refers to the framework and services that provide the following:

- generation, production, distribution, control, revocation, archive, and tracking of public key certificates;
- management of keys;
- support to applications providing confidentiality and authentication of network transactions
- data integrity; and
- non-repudiation.

The PKI encompasses "Certificate Management" and "Registration" functions, as well as "public key enabled applications."

The target DoD PKI shall provide an integrated public key infrastructure that supports a broad range of commercially based, security enabled applications and provides secure interoperability with the DoD and its federal, allied and commercial partners while minimizing overhead and impact to operations. It is the objective of the DoD PKI to provide certification services that have the following characteristics:

- Standards-based,
- Support multiple applications and products,
- Provide secure interoperability throughout the DoD, and with its partners such as other Federal government agencies, allies and industry, and academia,
- Support digital signature and key exchange applications,
- Support key/data recovery,

- Commercial-based, allowing for outsourcing of elements, as appropriate, and
- Support Federal Information Processing Standards (FIPS)-compliance requirements.

It will be developed in accordance with the DoD's Defense in Depth, layered Information Assurance (IA) strategy. It will support two assurance levels, Class 4 and Class 5, for the protection of unclassified information or additional protection of information on classified networks and the protection of classified information in an open environment, respectively. To achieve these objectives, the target DoD PKI will apply layered security, e.g., operating the PKI as appropriate on protected and unprotected networks, which will enable the DoD to minimize Government Off-The-Shelf (GOTS) developments and leverage existing commercial PKI technology, standards, and services.

On 6 May 1999, the Deputy Secretary of Defense issued a memorandum (Reference B) which encouraged the widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. It stated that the DoD PKI will initially support three levels of assurance, defined as Classes 3 and 4 (formerly Medium and High) for the protection of unclassified/sensitive information, and Class 5 (for the protection of classified information on unencrypted networks). The long-term goal is to provide a Class 4 certificate to everyone within the DoD and where appropriate Class 5 certificates via the target DoD PKI starting in January 2002. On 6 May 1999, the Deputy Secretary of Defense issued a memorandum (Reference B) which encouraged the widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. It stated that the DoD PKI will initially support three levels of assurance, defined as Classes 3 and 4 (formerly Medium and High) for the protection of unclassified/sensitive information, and Class 5 (for the protection of classified information on unencrypted networks). The long-term goal is to provide a Class 4 certificate to everyone within the DoD and where appropriate Class 5 certificates via the target DoD PKI starting in January 2002. Each assurance level has its own set of requirements for technical implementation and process controls, which becomes more rigorous as the level increases.

The DoD Certificate Policy defines the applicability of these assurance levels for the protection of information based on its value or sensitivity, the risk and the consequences of loss, disclosure or modification. The security requirements in the Certificate Policy will be incrementally increased over time to increase the security posture of the Department in a cost-effective manner. The planned / incremental changes will be documented in a companion planning document and published along with the CP to allow developers some insight into future security requirements. The CP for the target PKI will be an updated version of the current CP.

The target DoD PKI employs centralized certificate management and decentralized registration, and uses common processes and components to minimize the investment and manpower to manage and operate the PKI.

The strategy to achieve the target DoD PKI is intrinsically linked to the overall DoD strategy for achieving IA. Key to the successful implementation of both strategies is the ability of the Department to immediately begin leveraging the existing IA capabilities

afforded by commercial technology. The DoD PKI strategy recognizes that traditional GOTS based implementations will not be able to keep pace with an IA strategy based on commercial technology and services. It recognizes that the DoD PKI must, to the greatest extent possible, employ an open standards approach based on commercial products and services that can keep pace with technological rollover and the constantly evolving applications and standards inherent in the information technology (IT) environment. It must do this while still maintaining the appropriate levels of security for the information being protected.

Notwithstanding this need for a commercially-based acquisition model, the DoD PKI strategy recognizes and takes into account, the relatively immature state of commercial PKI products and standards. This translates into potential operational, cost or schedule risks requiring workarounds to satisfy necessary security and operational functions and by definition, implies an incremental, evolutionary approach to achieving the target DoD PKI. The ability of the DoD to address this issue is largely dependent on the success of the DoD Strategy Information Assurance Framework and specification initiatives, designed to foster the incorporation of DoD-required capabilities into commercial IT products and services.

This document establishes the enterprise-wide end-state for the DoD PKI and outlines the DoD strategy and timeline for the availability of PKI capabilities. In addition, it assigns roles and responsibilities and highlights critical issues and challenges that must be addressed concurrent with the implementation of the strategy.

1. Introduction

The Department of Defense (DoD) Key Management Infrastructure (KMI) is the critical underpinning of the Department's IA capabilities and is a vital element in achieving a secure IA posture for the Defense Information Infrastructure (DII). Accordingly, it is imperative that the Department takes an aggressive approach in acquiring a KMI that meets the requirements for all IA services. The DoD KMI is responsible for provisioning cryptographic key products, symmetric keys as well as public keys, and services for military, intelligence, governments, allied, contracting and business customers. The DoD Public Key Infrastructure (PKI) is an essential element and a major component of the KMI.

PKI, as defined herein, refers to the framework and services that provide for the generation, production, distribution, control, and tracking of public key certificates. It provides the critically needed support to applications providing secure encryption and authentication of network transactions as well as data integrity and non-repudiation. Recognizing that PKI technology is still immature and changing rapidly, the DoD's strategy is to pursue early adoption of technology and services. It will actively participate with industry to obtain the detailed technical understanding needed to fully specify requirements resolve standard issues and accelerate industry wide convergence to a purely standards-based, interoperable capability which is not dependent on vendor-specific capabilities or technologies.

This document establishes the enterprise-wide end-state for the DoD PKI and outlines the DoD strategy and timeline for the availability of PKI capabilities. In addition, it assigns roles and responsibilities and highlights critical issues and challenges that must be addressed concurrent with the implementation of the strategy.

1.1 Public Key Enabled System Elements

Three elements of a public key enabled system must work together to achieve secure functionality: certificate management, registration, and public key enabled applications (*Figure 1*).

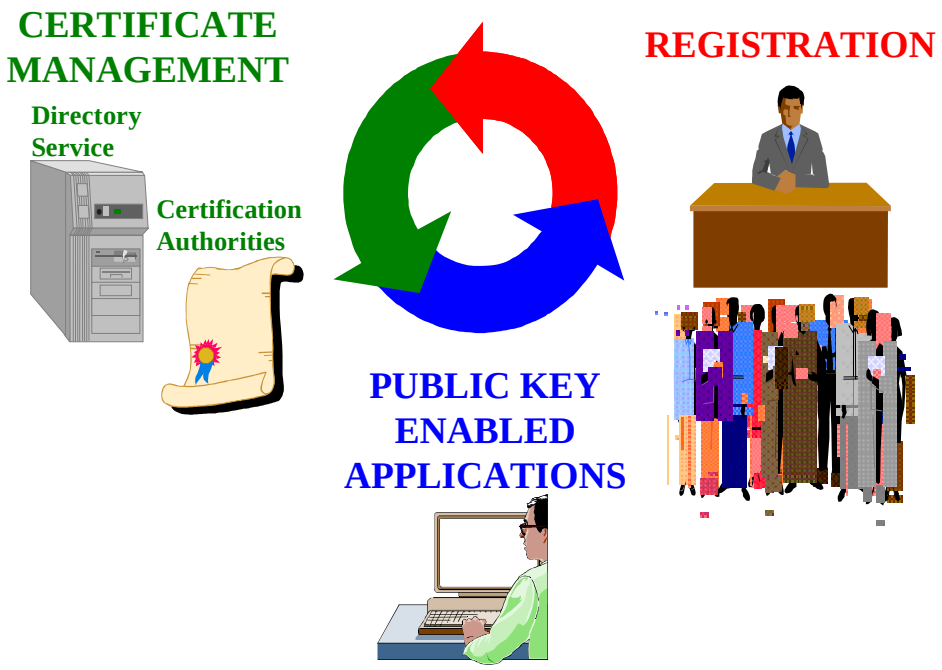

Figure 1. Public Key Enabled System

1.1.1 Certificate Management

Certificate Management involves the generation, production, distribution, control, tracking and destruction of public/private keys and associated public key certificates. Certificate Management is composed of Certification Authority (CA) and Directory Services. Central to the certificate management element is a trusted third party that certifies the identity of the possessor of a private key used for digital signature or key exchange. Certification Authorities (CAs) serve as trusted third parties and provide digitally signed certificates for users and components.

Certificates are the instruments used to convey trust. The DoD PKI will issue signature certificates and encryption certificates. The DoD PKI will support key recovery for private keys associated with encryption certificates to support data recovery. To achieve common certificates across the entire DoD, the DoD PKI identity and encryption certificates will have a minimum/common set of attributes as stated in the certificate profile section of the US DoD X.509 Certificate Policy (Reference A) (e.g., citizenship, government / non-government employee, service, or agency affiliation). Additionally, some DoD programs such as the Defense Message System (DMS) will require attribute certificates.

Information contained in the certificate includes a public key, a version number, the issuer's name, a serial number, the individual's (or end entity's) name, public key, validity period for use and optionally other attributes or privileges. An end entity can be either a person or a component such as a computer or application. Within the DoD PKI, the certificate management process is responsible for:

- Digitally signing each certificate, thereby certifying the association of the public key to the corresponding end entity;

- Managing the revocation of certificates. DoD will use two methods to manage the revocation of certificates: (1) Publishing and posting a Certificate Revocation List (CRL) to the directory, and (2) Providing a mechanism for a real-time check of the revocation status;

- Archiving required certificate management information (e.g. registration information, certificates, CRLs, etc.), to support non-repudiation of digital signatures (for at least the period of time defined in the CP); and

- Providing tools and procedures for personnel responsible for user registration.

The Directory Services portion of the Certificate Management element is used to make certificates and CRLs available to the applications. In addition to making certificate information available, directories can be used to make other end entity information available such as e-mail address, phone numbers, postal address, etc.

1.1.2 Registration

The registration process requires agents, Registration Authorities (RAs) with software tools, recognized by the infrastructure. They are responsible for authenticating the identity and any additional long term attributes of the end entity for the CA, as well as registration of the users' Distinguished Names. Certificates may also contain additional information and it is the responsibility of the RA to verify the accuracy of this information. The requirements for the RAs and associated tools are defined in the US DoD X.509 Certificate Policy.

1.1.3 Applications

The PKI supports the employment of cryptographic security services by providing valid public key certificates and CRLs to cryptographic aware applications. The user's (end entity's) cryptographic aware applications actually encrypt and decrypt data and/or sign and verify signatures. Encryption and digital signatures can provide the following: confidentiality, integrity, non-repudiation, and authentication. To use public key technology, application developers must understand the supporting infrastructure's policies, usage, and interfaces. There are a growing number of applications today which come ready off-the-shelf to accept PKI certificates. Because of the newness of the standards and products, however, there can be some functional and interoperability problems between vendors' products. The Defense Information Systems Agency (DISA) and National Security Agency (NSA) are actively working with the vendors and the standards communities to achieve standard specifications and implementations to improve interoperability. The DoD will ensure that these DoD specifications are consistent with the emerging commercial and National Institute of Standards and Technology (NIST) Federal standards to support DoD interoperability requirements. The DoD PKI program will continue to track new and evolving Internet Engineering Task Force (IETF) standards to ensure the most viable commercial standards are fully leveraged to support maximum interoperability in the future. The Assistant

Secretary of Defense for Command, Control, Communications and Intelligence (ASDC3I) is in the process of issuing a separate policy on PKI applications.

1.1.4 Defense in Depth

The DoD PKI is a critical component of the Department's IA Strategy, which is predicated upon a "Defense in Depth" construct. It involves a series of layered defenses of varying strength and assurance levels, deployed so as to provide multiple roadblocks between our sensitive information systems and those internal and external adversaries who would try to exploit them. The implementation of the IA Defense in Depth construct involves directing DoD's Protect, Detect, and Respond initiatives at several critical focus areas (layers) within the DoD's Information Technology environment to include:

- The Wide Area Networks (WANs) that are used to interconnect DoD systems, and those of its allies and trading partners, to ensure the confidentiality of DoD communications and protect against Denial of Service (DoS) attacks that could disrupt DoD's ability to communicate prior to or during operational deployments.

- The boundary points at which DoD LANs connect to these WANs by deploying boundary protection measures to control and monitor access to the internal LANs.

- The hosts, servers, applications, and operating systems used with DoD LANs.

- The system that will detect, analyze and respond to unwarranted intrusions at local, regional and national levels and which provide the ability to correlate and fuse data.

- Key Management Infrastructure (KMI) services. The DoD PKI is a subset of the KMI, which also includes the Department's traditional key management systems, the Electronic Key Management System (EKMS) and physical products such as codebooks and authenticators.

The IA Strategy recognizes that no single element or focus area can provide adequate assurance independent of the other focus areas, and that the focus areas must be linked to create an adequate security posture for the Department.

The IA Strategy provides the IA Framework and supporting specifications which form the basis of Department-wide acquisition guidance delineating the security criteria and compliance testing that new information technology (IT) products/services must meet in order to be procured for use within the DoD. Security testing to validate that the new IT products meet the mandatory IA criteria must be performed by NSA, or a commercial IA test facility which has been accredited by NSA and National Institute of Standards and Technology (NIST) pursuant to their National Information Assurance Partnership (NIAP). Results of NSA and/or NIAP accredited lab IT testing will be published on a NSA Comparative IA Products List.

2. Target DoD PKI

2.1 Target Objectives

The target DoD PKI shall provide an integrated public key infrastructure that supports a broad range of security-enabled applications, and supports secure "cost effective" interoperability with DoD and its federal, allied and commercial partners while minimizing degradation to operations. It is the objective of the DoD PKI to provide certification services that have the following characteristics:

- Standards-based,
- Support multiple applications and products,
- Provide secure interoperability throughout the DoD, and with its partners such as other Federal government agencies, allies and industry, and academia,
- Support digital signature and key exchange applications,
- Support key/data recovery,
- Commercial-based, allowing for outsourcing of elements, as appropriate, and
- Support Federal Information Processing Standards (FIPS)-compliance requirements.

The target DoD PKI will be developed in accordance with the DoD's Defense in Depth layered assurance, IA Framework strategy. It will support two assurance levels, Class 4 and Class 5, for the protection of unclassified information or additional protection of information on classified networks and the protection of classified information in an open environment, respectively. In order to achieve these objectives, the DoD target PKI will apply layered security, e.g., operating the PKI as appropriate on protected and unprotected networks. This will enable the DoD to minimize GOTS developments and leverage existing commercial PKI technology, standards, and services.

On 6 May 1999, the Deputy Secretary of Defense issued a memorandum (Reference B) which encouraged the widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. It stated that the DoD PKI will initially support three levels of assurance, defined as Classes 3 and 4 (formerly Medium and High) for the protection of unclassified/sensitive information, and Class 5 (for the protection of classified information on unencrypted networks). The long-term goal is to provide a Class 4 certificate to everyone within the DoD and where appropriate Class 5 certificates via the target DoD PKI starting in January 2002. Each

assurance level has its own set of requirements for technical implementation and process controls, which becomes more rigorous as the level increases. The US DoD X.509 Certificate Policy defines the applicability of these assurance levels for the protection of information based on its value or sensitivity, the risk and the consequences of loss, disclosure or modification.

The current US DoD Certificate Policy defines the requirements for the current DoD PKI implementations for Class 3 and Class 4. The security requirements in the Certificate Policy will be incrementally increased over time to increase the security posture of the Department in a cost-effective manner. The planned / incremental changes will be documented in a companion planning document and published along with the CP to allow developers some insight into future security requirements. The CP for the target PKI will be an updated version of the current CP.

Classes 3 and 4 have been defined (Reference A) to support the protection of non-classified mission critical, mission support, administrative or format sensitive information on open networks (i.e., unencrypted network). These PKI Classes can also be used on closed networks (i.e., encrypted system high networks such as SIPRNET) to provide additional protection such as user authentication and data separation / communities of interest (COIs). The Class 4 PKI service will be used to protect sensitive or unclassified mission critical information in a high-risk environment such as the NIPRNET. For other applications, including many business transactions and protection of sensitive or unclassified administrative information, a Class 3 PKI is appropriate. Class 5 will be used for the protection of classified information on open networks or in other environments where the risk has been determined to be high.

KMI support for these Class 5 applications is currently provided by the Electronic Key Management System (EKMS). These key services, as well as the newer PKI services, will be part of the unified DoD Key Management Infrastructure. NSA, in conjunction with DISA, the Services and industry partners, is currently defining the strategy that merges EKMS, PKI and other relevant key management initiatives. The target PKI described in this document will be consistent with and build upon the KMI strategy initiative. .

2.2 Target Architecture Overview

The target DoD PKI employs centralized certificate management and decentralized registration, shown in Figure 2, and uses common processes and components to minimize the investment as well as the manpower required to manage and operate the PKI.

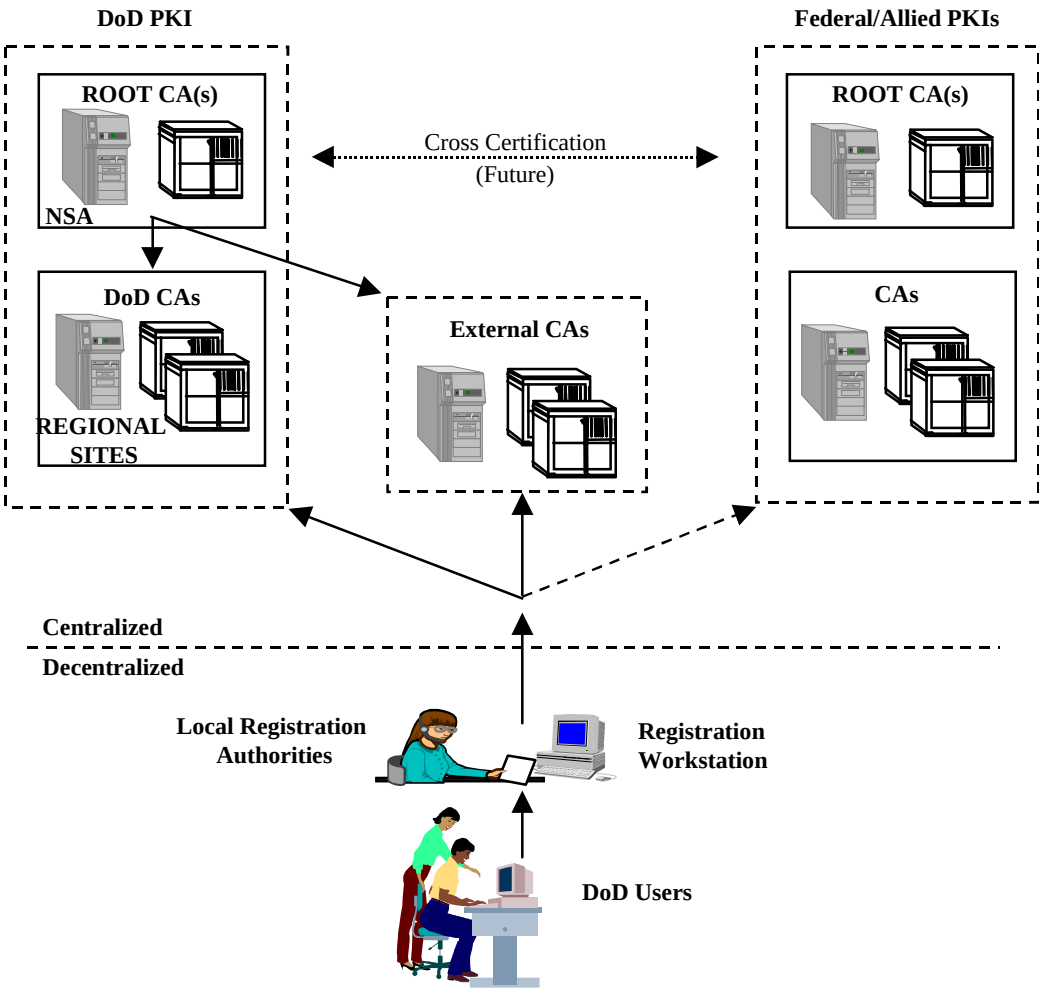

Figure 2. Target DoD PKI CA Architecture

2.2.1 Target Certificate Management

Certification Authorities

The centralized portion of the certificate management process, shown in Figure 2, is comprised of a combination of DoD owned and operated components (the DoD Root CA(s) and CAs in the DoD PKI box). The DoD will manage and operate its Root CA(s). The Root CA(s) are responsible for managing subordinate DoD CAs- and External CAs (ECAs) and cross certifying with other domains for interoperability. The Root CA(s) will be operated as offline devices with maximum physical, personnel and procedural security protections. A standards-based certificate request format (e.g. PKCS #10 (Reference E) or RFC 2511 (Reference F)) will be used to interface with the Root CA(s) and register subordinate CAs into the system in a "trusted" out of band process.

Based on current technology limitations, it is envisioned that the DoD will require separate CAs on each of its networks (e.g Top Secret, SIPRNET, NIPRNET) similar to the

current implementations today where identical PKIs are replicated on each network. The DoD CAs that support classified, mission critical, command and control applications will be under the direct control of the DoD Root CA(s) and will be owned and operated by the DoD. These are shown in the DoD PKI box (Figure 2). They are networked devices supporting a standards based secure interface for the Local RAs for user registration. They will be operated with the technical, physical, personnel, and procedural security protections as defined in the target US DoD X.509 CP. It is expected there will only be a small number of CAs located at several regional sites. If it is determined to be necessary due to cost, performance, and/or availability, CAs could be placed in the Pacific and European theaters in addition to the ones located in the continental US.

Registration Authorities

The registration function is decentralized in the target DoD PKI with RAs responsible for user identification. The DoD Services and Agencies will manage registration. The target DoD PKI user registration process is shown in Figure 3. It depicts a common workstation and web-based application with hardware token (FIPS 140-1 certified). A common registration workstation with unified ordering and delivery software will be based on commercial standards and technologies. The target envisions a common set of processes and tools so that the only differences between assurance levels from the RAs' and users' perspective are the user identification procedures and tokens protecting the keys. This will allow DoD users to register with the appropriate CA server through a single RA. This single registration workstation should be able to transparently register users into DoD CAs, commercial certificate service providers or other external CAs as needed.

End Users

End users commonly referred to as end-entities can be a person, a machine such as a router or a process running on a computer such as a firewall. The target PKI will need to provide support for all end entities including non-human. Registration of end entities will use a common registration application to securely register with the infrastructure. During registration, the user's token will generate a digital signature key pair (public and private key) and send the public key to the CA. Once the certificate is returned by the CA, the user can then load the certificate onto the token (e.g., smartcard, Universal Serial Bus (USB) device, or personal computer (PC) card). The Department of Navy has the overall responsibility to define the PKI token for the Department. It is envisioned this token and certificate can be used in a variety of applications. Once the user has a digital signature certificate, he/she can use that certificate to request additional certificates such as encryption or attribute certificates at the same assurance level.

Outsourcing

To minimize investment and overhead costs, the target architecture will be designed to allow for outsourcing of selected PKI services. Applications for potential outsourcing include the protection of unclassified mission support, format sensitive, administrative, and selected mission critical data. Commercial service providers who meet the security / functional requirements and are more cost effective than a DoD managed and operated system will be considered for outsourcing services. If commercial solutions do not meet all

of the assurance requirements in the higher classes, the government will continue to develop, procure, and operate some portion of the infrastructure.

Tactical Support

The DoD PKI will support tactical users / applications. The proposed target architecture will address and support tactical requirements. However, the target architecture requires network connectivity to the regional CAs. If this connectivity becomes an issue, the target architecture will allow the CAs to be deployed on local tactical networks to meet mission needs where communications or time limitations do not allow for connection back to the regional sites. Among the things necessary to make the PKI more viable in the tactical environment are policies and procedures, applications and PKI services adapted to that environment.

Interoperability

The DoD target PKI plans to eventually achieve secure interoperability with non-DoD entities through a process called "direct cross certification," which establishes a policy and process for recognizing third party CAs, or through an evolving concept like the Federal Public Key Infrastructure (FPKI) "Bridge Certification Authority" (Reference D). Near term, vendors and contractors, will be using External Certification Authorities (ECAs) for interoperability with DoD. ECAs will be established through a process that ensures a commensurate level of trust with the DoD PKI. ECAs will be approved by the DoD Chief Information Officer (CIO), in coordination with the DoD Comptroller and the OSD General Counsel.

Although the target DoD PKI envisions secure interoperability with Federal/Allied PKIs through direct cross certification or through evolving concepts like the FPKI "Bridge Certification Authority", for a variety of reasons, DoD users may have to be registered into multiple infrastructures. As an example, DoD users may have to be registered into allied infrastructures due to political and sovereignty issues. The goal is to use the same tools and procedures as in the normal registration process whenever possible. Several international working groups have been established to work on interoperability and PKI related issues. The DoD will actively participate and attempt to influence those activities to avoid non-interoperable solutions or solutions which do not meet the Department's security needs.

Directory Services

Although not depicted in Figure 2, Directory services are a critical element of certificate management, and as such, constitute a key component of the target DoD PKI. Within the certificate management context, directories are used as a repository for the distribution of certificates and CRLs. The target DoD PKI calls for a "common" DoD-wide directory to support all DoD public key enabled applications. The target directory system will allow multiple communication options and client access protocols. The security features shall be configurable to include digital signature for strong identification and authentication (I&A) as well as non-repudiation of administrator actions. In some environments, the confidentiality requirements will dictate the use of a transport or network layer encryption service such as Transport Layer Security (TLS).

Attack Sensing, Warning and Response Services (ASW&R)

Although not depicted in Figure 2, Attack Sensing, Warning and Response (ASW&R) services are a critical element in the protection of the certificate management infrastructure, and as such, constitute a key component of the target DoD PKI. At a minimum, it will be used to protect the DoD operated centralized portions of the PKI. Many current authors refer to cyber-ASW&R with the shorthand term of "intrusion detection." ASW&R systems and technologies employed in the target PKI are intended to counter a sophisticated, structured and extensively funded threat. This threat could make use of organized methods, a professional cadre of operatives, and with access to all-source intelligence whose long-term goals are to disrupt, modify or thwart the interests of the United States Government or its allies.

Technology Forecasting

Although the PKI market is still relatively immature, it is rapidly moving from the developmental stage of pilot programs to one in which it is integrated as a key component of the IT infrastructure in many organizations, including the DoD. Its deployment continues to be limited, however, because of the complexity of the technology, the cost and its integration into applications. X.509-based digital certificates will continue to be the core security enabler of electronic commerce and other security services on public networks. Security policy issues remain to be solved in the areas of cross-certification and certificate revocation. It can be expected however that in the next 4 to 5 years, the technology and standards will mature and be able to provide interoperable solutions across vendor products and services (Reference J). The DoD will continue to monitor activities in the PKI arena.

2.2.2 Target Registration Concept

The target user registration concept employs pre-registration and direct delivery of the certificate and key information to the end user (or equipment). As an example, one potential implementation is the following: the RA making use of this common web-based registration application securely authenticates (e.g., SSL) to the appropriate CA servers via a common KMI management front end and registers the user(s) (1). Next the RA identifies the user as required by the policy and provides the necessary information for the user to authenticate to the CA server (2). The CP specifies the authentication requirements/process for the various assurance levels. After receiving the authentication information, the user can use a common registration application to securely connect to the appropriate CA server and request a certificate (3). During registration, the user's token or software application will generate a digital signature key pair (public and private key) and send the public key to the CA server (4). The CA server processes the request, verifies possession of the private key, generates the certificate, posts it to the directory system and returns the certificate to the user (5). The user can then load the certificate onto the token (e.g., smartcard, Universal Serial Bus (USB) device, or personal computer (PC) card). This token / certificate can be used in a variety of applications (6), allowing a single registration to support multiple applications. Once the user has a digital signature certificate, he/she can use that certificate to request additional certificates such as encryption or attribute certificates at the same assurance level.

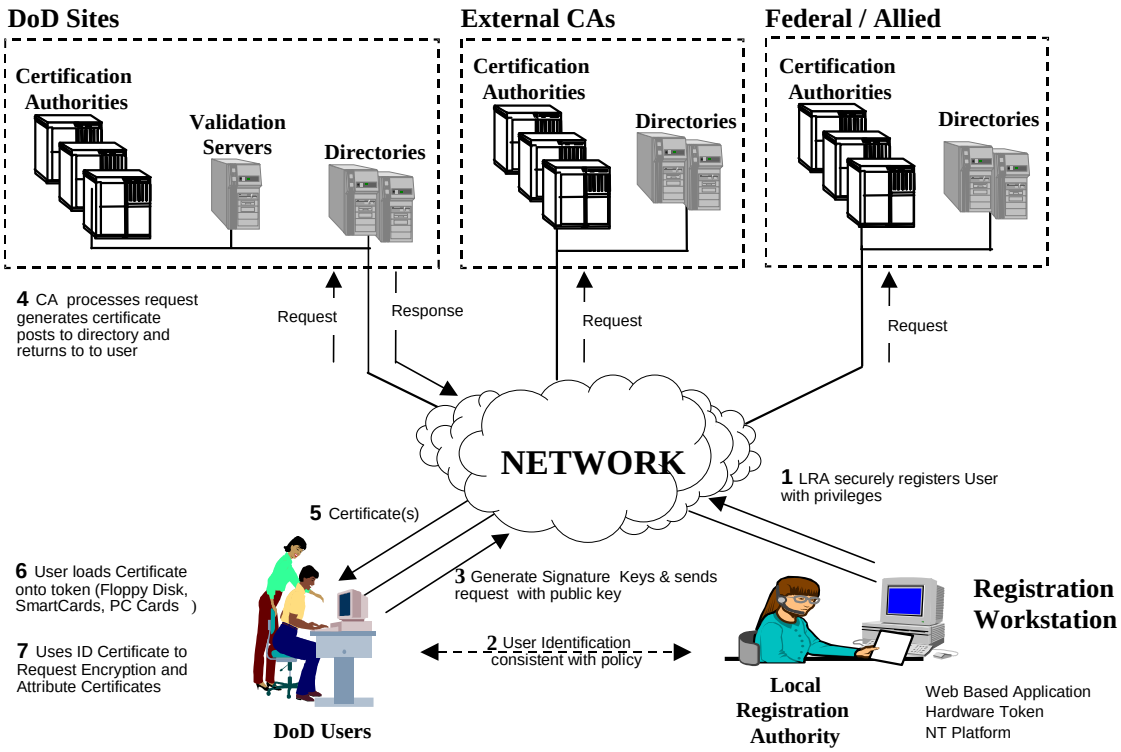

Figure 3. Target User Registration Process

The DoD PKI will support the recovery of decryption keys for information as it traverses the network and while at rest. The key recovery mechanisms used in the DoD PKI will comply with the future FIPS for key recovery products. Additionally, a Key Recovery policy will be issued for DoD-wide implementation. NSA has already prepared preliminary criteria for the evaluation of key recovery systems. Until the Key Recovery FIPS is finalized these criteria will be used to assess prospective applications that provide confidentiality services, i.e. encryption of data.

3. Strategy to Achieve Target

As mentioned earlier, the successful deployment of the DoD PKI is linked to the availability of the other IA focus area technologies in the "Defense in Depth" layered assurance construct. Accordingly, the strategy to achieve the DoD PKI must be linked to the overall DoD strategy for achieving IA. Key to the successful implementation of both strategies is the ability of the Department to leverage the existing IA capabilities afforded by commercial technology. This ability is predicated upon both the availability of product assessment criteria against which the security functionality of products can be independently tested and validated and the existence of appropriate architectural guidance to support the configuration of these products into security solutions.

DoD's Defense in Depth, IA Strategy mandates creating an overarching technical framework that provides the architectural guidance for successful application of the layers. This framework is augmented by a series of technical specifications delineating the technical, performance, and best practice standards for each of the Defense in Depth layers. These technical specifications are further supported by a series of security specifications for each of the technologies/IA products and services specified within the focus area technical specifications. These security specifications, called Protection Profiles, are written in accordance with the International Common Criteria for Information Technology Security (Reference G), and will serve as the basis against which IA products/services can be assessed and evaluated to determine their appropriateness for use in securing DoD systems.

Consistent with the IA Strategy, the DoD PKI Strategy is designed to immediately begin leveraging the existing capabilities and services afforded by the commercial PKI industry. Using the IA Framework and supporting technical and security specifications, the DoD will promulgate the architectural guidance for the target PKI described in this Roadmap. The technical specifications also include the applicable policy documents/guidance required for consistent implementation of policy, procedures, and practices to ensure secure operation of the PKI. These are essential to providing DoD users and industry the standards necessary to develop and deploy the target PKI. Security testing to validate that new IT products meet the mandatory IA criteria must be performed by NSA or a commercial IA test facility which has been accredited by NSA and NIST pursuant to NIAP.

The DoD PKI Strategy recognizes that a traditional, GOTS-based implementation will not be able to keep pace with an IA strategy based on commercial technology and services. It recognizes that the DoD PKI must employ an open standards approach, based on commercial products and services that can keep pace with the technology rollover and constantly evolving applications and standards inherent in the IT environment, while still maintaining appropriate levels of security. The DoD PKI must be able to interoperate securely both within the DoD and externally with its Federal and international counterparts

and trading partners. This translates to an acquisition model that includes outsourcing consistent with maintaining appropriate levels of security.

Notwithstanding the need for a commercially based acquisition model, the DoD Strategy must also recognize and take into account the relatively immature state of commercial PKI products and standards, and employ an incremental evolutionary approach to achieving the DoD PKI. Accordingly, the target DoD PKI will be designed with adequate flexibility to ensure that it can evolve over time. It will immediately leverage existing commercial capabilities in the baseline implementation and incrementally evolve the capability as commercial technology matures. The strategy mandates significant DoD involvement in commercial standards bodies to influence the direction and maturation of technology to address DoD PKI target requirements.

The majority of activity to date in the DoD PKI arena has focused on understanding the technology, the standards, operational policy and procedural issues, and establishing the role of PKI relative to the rest of the IA Defense in Depth model. The experiences gained from the two major DoD PKI initiatives, the development and deployment of an operational FORTEZZA PKI, in support of the Defense Message System (DMS) and other FORTEZZA-enabled applications, and the pilot medium assurance PKI, have been instrumental in the development of the target DoD PKI architecture. The decentralized FORTEZZA PKI, while based on GOTS technology and protocols, resulted in creation and understanding of a PKI technology baseline, development of the knowledge and expertise to influence commercial standards bodies, establishment of PKI policy and procedures, and an understanding and appreciation of their resultant operational impacts and issues. Similarly, the pilot medium assurance PKI serves as an excellent "hands-on" learning tool and is providing an initial appreciation of the benefits and shortfalls of a centralized PKI architecture based on commercial technology, policy, and procedures. It has helped DoD influence applications developers in the direction of standards-based public key enabled applications. Both provide critical lessons learned to focus target DoD PKI development activities and resulted in instantiations of architectural and technical specifications and supporting policy and procedural documents. These will serve as the predecessors and starting points for creation of the target DoD PKI technical and policy specifications to be developed in support of the IA Framework.

Appendix B defines the process for requesting PKI Pilots within the DoD. While using the FORTEZZA and medium assurance initiatives as sources of lessons learned, the strategy for the target DoD PKI is not constrained to evolving either of those efforts to achieve the target DoD PKI. The strategy calls for focused efforts to develop the DoD PKI portion of the IA Framework as the basis for acquiring the "best of breed" commercial PKI products and services required for the target DoD PKI. Concurrent with PKI specification development, the DoD will continue to conduct operational pilot assessments focused on the products and services available today from leading commercial vendors. This will allow the DoD to understand the state of commercial PKI technology, validate the technical specifications, establish and validate the business case for an outsourcing acquisition model, and identify the functional and security gaps within the target DoD PKI in order to develop a realistic and viable evolution path. This allows an incremental, evolutionary approach to achieving the target DoD PKI, while concurrently addressing immediate operational and

security requirements and generating the data and analysis essential to establishing an initial DoD PKI target capability.

The DoD PKI will be designed to support open commercial interfaces, cryptographic standards, and protocols. It will support security-enabled applications that have been designed to support the same open interfaces, cryptographic standards and protocols. These interfaces specifications, cryptographic standards, and protocols will be defined in the IA Framework technical specifications (Reference H) for both the PKI and applications focus areas. It will be incumbent on the DoD to only implement applications conformant to these specifications. Any application failing to comply with these specifications will not be supported by the target DoD PKI.

The target DoD PKI strategy implementation plan consists of the following critical milestones:

1. Creation, coordination, and promulgation of the DoD PKI and Applications portions of the IA Framework and supporting technical specifications and protection profiles, which will serve as the basis of Department-wide acquisition guidance for applications and DoD PKI products and services. The documents to be created include:

    a. The IA Framework chapter on PKI ;

    b. The IA Framework chapter on Applications;

    c. The Certificate Policy consistent with the companion planning document for the target DoD PKI;

    d. The technical specification for the DoD PKI, highlighting interoperability, cryptographic interfaces, standards, and protocols, key recovery, etc;

    e. The technical specification for security enabled client processing of certificates and CRLs;

    f. Protection Profiles for

        1) Certification Authority technology,

        2) Registration Authority,

        3) Directory,

        4) Clients,

        5) Key Recovery; and

        6) On-line Validation servers.

    g. Compliance criteria and test methodology for Protection Profiles.

2. Establishment of a Policy Management Authority to provide CP oversight and modification responsibility and authority (draft Policy Management Authority (PMA) attached in Appendix A).

3. Establishment of NSA and/or NIAP test capability to validate commercial PKI products and services against technical specifications and Protection Profiles.

4. Establishment of ECAs, for interoperability with DoD partners. The DoD PKI Program Management Office will use ECAs to provide security, functionality, interoperability, scalability, logistics, policies, procedures, ease and speed of deployment, and cost benefit analysis data.

5. NSA security assessments of leading commercial PKI technologies and service providers.

6. FORTEZZA PKI services and medium assurance operational security enabled IT pilots pending the availability of the initial target PKI capability to address immediate operational requirements for selected DoD applications (see Appendix B).

7. Gather and document requirements from the tactical user community. Analyze the requirements to verify the usability of the target architecture in the tactical environment. Conduct tactical pilots in order to verify the implementations meet the requirements.

8. Analysis of information obtained from DoD PKI activities in order to finalize the DoD Target PKI architectural, policy, and acquisition strategy decisions. This analysis must answer the following questions:

    a. What PKI services are not candidates for outsourcing consideration?

    b. Has DoD adequately leveraged industry away from vendor-specific implementations and accelerated convergence within the marketplace to standards-based implementations?

    c. Does DoD know enough to intelligently specify what it wants to buy?

    d. Will outsourcing portions of the DoD PKI services be more cost effective than operating them internally?

    e. Can our immediate operational and security requirements be satisfied?

9. DoD Target PKI competitive acquisition using results of 8. This may include the establishment of a contract for services with a commercial service provider as well as an acquisition to select CA technology (or technologies) to form the basis of a Government-operated portion of the target DoD PKI. Selected source must demonstrate ability to retain currency with technology rollover and new applications.

10. Establish a unified DoD KMI that merges EKMS, PKI and other DoD key management initiatives. The future KMI strategy will be consistent with and build upon the target described in this document. KMI Capability Increment 1 will include the Target DoD PKI.

The timeline / milestones for the target PKI strategy is shown in Figure 4. Appendix D contains additional milestones for deployment of the target PKI's registration capability and required usage within the DoD. The DoD PKI Implementation Plan contains the complete list of tasks required to meet these high level milestones (Reference I).

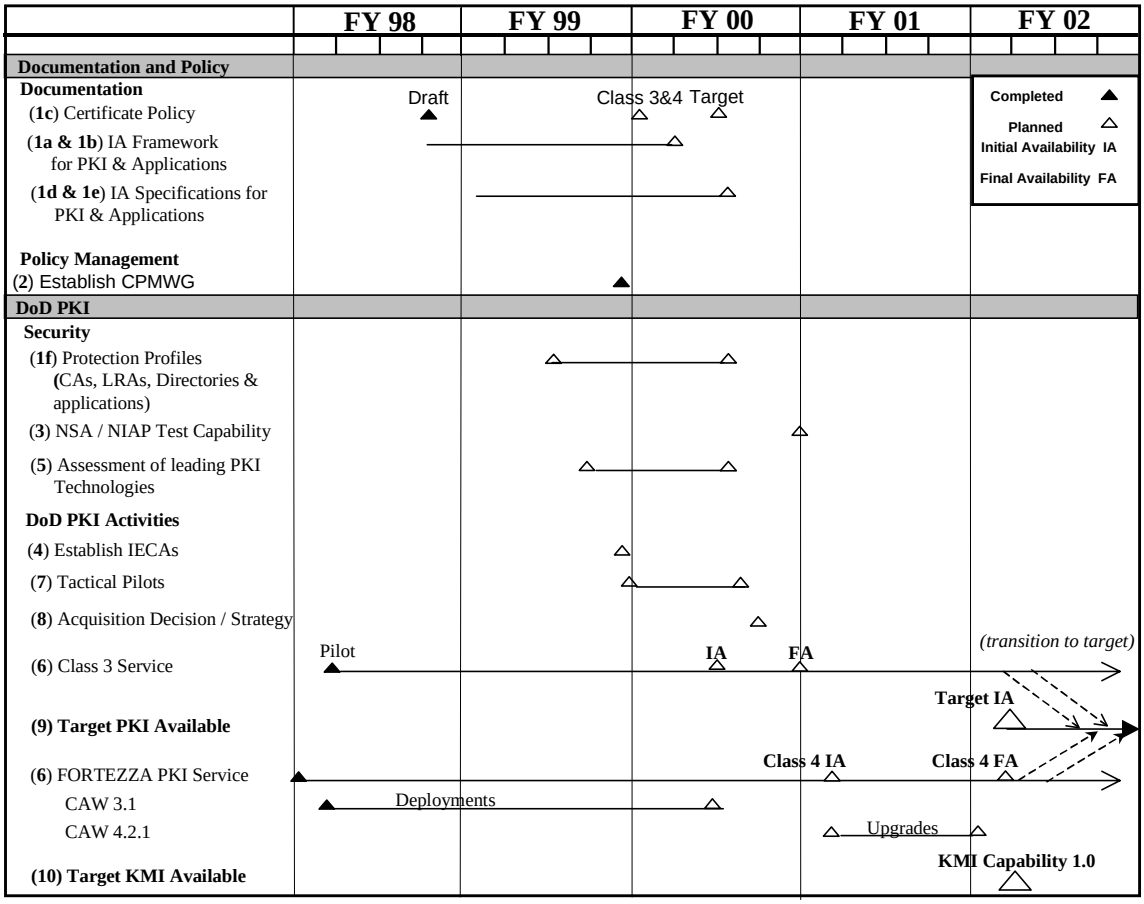

Figure 4. Schedule

4. Issues

This section identifies the policy and technical issues involved in developing and fielding the target DoD PKI.

4.1 Transition Issues

The transition to the target architecture will be evolutionary, as standards and technologies in the PKI area are not yet stable. The DoD is collecting much of the information necessary to make final decisions on the exact process for achieving the target architecture. Available technology and lessons learned from the current PKI activities (pilot medium assurance and FORTEZZA PKI efforts) will be inputs into the transition process. Both the medium assurance and FORTEZZA PKIs will be maintained and service will be continuous until all users are transitioned to the target PKI. Interoperability between the target and the current implementations will be required to allow for a smooth transition to the target as opposed to a hard cutover.

4.1.1 Funding

Funding for the DoD PKI will be shared between the NSA, DISA, Services and Agencies according to their responsibilities.

- The DoD PKI Program Management Office will identify resources to complete the development of the target architecture, perform the security analysis and testing of the system and components and procure and operate the Root CA(s).

- The DoD PKI Program Management Office will identify resources to integrate, implement and operate the centralized infrastructure components, the centralized CA Servers and Directories.

- The DoD PKI Program Management Office will assist the Services and Agencies in identifying resources to procure the local infrastructure elements and applications starting in FY99. The Services and Agencies must also identify manpower to operate, or funds to outsource, the operation of the local registration components and directories.

4.1.2 Architecture Extensions

This roadmap defines a unified PKI to support DoD-wide secure interoperability. Because of requirements such as special access programs and coalition interoperability, it will, in all probability, be necessary to also use a limited number of dedicated, specialized PKIs. The Office of the Assistant Secretary of Defense for Command, Control,

Communications, and Intelligence (OASD (C3I)) must validate the requirements for special PKIs and develop a management philosophy for these infrastructures.

4.2 Technical Risks

The target DoD PKI and IA Strategy are predicated on the availability of acceptable COTS products and services. Public key technology and commercial application standards are still immature and evolving. This leads to increased technical risk that the DoD will not be able to meet its operational requirements, and that it will have cost and schedule impacts. Areas of technical risk include, but are not limited to the following:

4.2.1 Application Processing

The security afforded by public key certificates depends not only on how they are generated and managed, but also on the end-user's applications processing and operating system security. None of the PKI applications currently on the market fully supports the target DoD PKI requirements. This is primarily due to the lack of accepted PKI standards resulting in a series of product-specific solutions tailored to specific markets that do not have the DoD's applicability requirements. Unfortunately, the DoD does not control the speed of the standards or their implementation into products.

Among the application's potential near-term shortfalls are revocation handling, data recovery, certificate extensions processing, certificate policy enforcement, path processing, algorithm interoperability, and cross-certification. The lack of high assurance operating systems or applications at the user's fingertips increases the security risks. The effect is that, at least in the near term, the DoD PKI may not fully satisfy every operational and security requirement. Until the applications fully implement DoD requirements, approved procedures will need to be developed to gain the necessary security and operational functions.

4.2.2 Revocation Architecture

Revocation is an area of the technology that is not yet mature. Today there are two competing methods for compromise recovery notification being developed within the standards community. The first is a CRL and the second is on-line verification. There is a concern for the scalability of on-line verification and standards support. It is likely that both methods will need to be supported within DoD. On-line verifications require the DoD to acquire, manage, and operate on-line repositories in addition to directories. Applications may need to be developed to query on-line repositories. DoD activities are in the early stages of development for the infrastructure elements and policy necessary for on-line verification. These activities include participation standards activities, modeling and piloting some early commercial technology offerings.

4.2.3 Privilege

While public key certificates bind an identity to a public key, a need exists to bind privilege information to a particular owner. The current state of technology defines two privilege

management models. Both of these models are dependent upon their relationships with public key infrastructures. The "control" model requires both the privilege information and the control model to be highly distributed. The Defense Message System uses a subset of this model, whereby the privileges of the user are included as extensions to the key management certificate and the associated security policy is distributed to all the dependent messaging applications in the system. In contrast, the "delegation" model, primarily used by the banking/financial community, uses attribute certificates in a highly centralized environment. The attribute certificate delegation path is distinct from the certificate validation path used to validate the public key certificates of the entities involved in this delegation process. The issues that the DoD must address in designing and deploying a privilege management infrastructure include determining which model is appropriate. The evaluation of the operational requirement, the available and emerging technologies, and the ease of implementation must be done across the entire DoD. The solution sets must scale across organizational as well as geographical domain boundaries, and, must be scalable across multiple applications.

4.2.4 Interoperability

The DoD PKI must interoperate with a large number of other PKIs, including those of allies, commercial partners and the rest of the Federal government. The approach of basing the target DoD PKI's design on commercial standards, algorithms, and protocols may result in interoperability with commercial trading partners, yet still fail to achieve interoperability with non-U.S. entities, e.g., Allies and Coalition partners. These other PKIs may be based on different products, policies, certificate policies, and algorithms. Proactive work by the DoD to identify critical government and allied programs for interoperability and to ensure that these programs use common standard algorithms and protocols will increase the likelihood of interoperability with partners.

4.2.5 Scalability

As a PKI becomes larger, some of the functions may not scale well. The technology is still evolving, and solid data does not exist that describe how increasing the number of users affects the characteristics of the PKI. Compromise recovery, key recovery, registration, and directory access and management are functions that may become progressively more expensive or less secure as the number of users increases. The DoD PKI Program Management Office will use the pilots, modeling and early deployments to identify scalability problems and work with vendors to find ways to improve the scalability of the solutions while maintaining (not degrading) the security services supported by the PKI.

DISA and NSA are developing a model to aid in the engineering, planning and programming, and testing of the DoD PKI system. This model will also be used to assess the impact of the DoD PKI on the telecommunication/network infrastructure. Multiple sets of performance data will be sampled at different frequencies and will be analyzed to assess the performance of the system during peak and average time periods. Performance reports, utilizing data collected from pilot efforts and automatic system performance reports will provide insight into the operational performance of the system for sizing and analysis purposes.

Analysis will continue to be performed to identify possible bottlenecks of the current system and ways to improve its performance. Scenarios such as user projections, stressed environments (i.e., crisis, wartime workloads), application projections, etc., will be modeled and performance data captured.

4.2.6 Directories

Currently, there are multiple directory efforts within the Department. The DoD PKI Program Management Office has the responsibility to ensure that the multiple directory systems are integrated into an interoperable directory infrastructure and architecture that can be used across the DoD. This is a critical service for public key-enabled technologies and represents an area of major cost if done in an unorganized fashion.

While the DoD target PKI allows the acquisition of a common, DoD-wide directory, capable of supporting the needs of the entire Department, it is being developed independent of any one specific application. The DoD must continue to work with federal government and allied partners as they evolve their directory systems to ensure security and interoperability.

4.3 Tactical Concerns

While the DoD PKI supports most tactical requirements through the use of local CA servers, there are still some issues concerning the completeness of the services provided by the local servers. Since the tactical environment does not always provide easy access to the infrastructure elements (e.g., CA Servers, directory), services requiring such access may suffer. These may include rapid mobilization, rapid compromise recovery required by tactical operations, key recovery, and support for remote end users. The Tactical DMS Working Group outlined a number of "operational considerations" for using FORTEZZA in the tactical environment. Among their concerns were: low bandwidth, MINIMIZE and radio silence, rapid addition of personnel, rapid changing of roles and granting of privileges.

5. Roles and Responsibilities

This section identifies the roles and responsibilities for implementing, operating, and managing the DoD PKI.

5.1 Program Management

NSA is responsible for overall program management of all DoD efforts required to execute this DoD PKI roadmap. DISA will provide the Deputy Program Manager, to be co-located with the Program Management Office (Reference C).

5.2 Requirements

5.2.1 Security

NSA is responsible for defining the security architecture and security criteria for the DoD PKI. This includes criteria for the components as well as their operation. NSA (or an approve NIAP vendor) will evaluate the security of products and services employed in the DoD PKI.

5.2.2 Functional and Operational

The PMO will coordinate with CINCs, Services, and Agencies to ensure that services required by users are available in a timeframe consistent with their needs.

5.3 Interoperability

The DoD PKI PMO will ensure that the DoD PKI is able to interoperate securely both within DoD and externally with Federal, NATO, partner nation, and business partners. The PMO must address technical challenges, as well as ensure that the necessary policies, practices and procedures are in place to advance interoperability.

5.4 Development

NSA will lead any required research and development efforts for the centralized certificate management PKI components and services, Root CA(s) and CA Servers. Additionally, NSA in conjunction with DISA, the Services and industry partners, will develop specifications for commercially produced PKI products and applications for use in the DoD pursuant to the IA Framework initiative.

DISA will lead integration of the centralized components, the CA servers and Directory components. Additionally, DISA will lead the development of the directory components and services.

Services and Agencies are responsible for PK-enabling their specific-developed applications. These applications must adhere to the target DoD PKI specifications to utilize the DoD PKI services. The PMO is responsible for providing technical guidance and support to programs and vendors in the development of PK-enabled applications.

5.5 Procurement

5.5.1 DoD PKI Program Management Office (PMO)

The DoD PKI PMO will procure, or direct the procurement of, the centrally operated infrastructure elements. The DoD PKI Program Management Office (PMO) will develop the acquisition strategy for the DoD PKI, the certificate management components and services.

5.5.2 Services, and Agencies

Services, and Agencies will procure local infrastructure elements, RA workstations, local directories and PK-enabled applications in accordance with the IA Framework PKI technical specifications and guidance.

5.6 Operations

The target allows for flexibility in management and operation of the DoD PKI components. Although placement of the centralized and decentralized components needs to be finalized the requirements for the management and operations are detailed in the DoD Certificate Policy. It allows CINCs, Services and Agencies to integrate the management and operation of the DoD PKI directory and registration components onto common platforms. CINCs, Services, and Agencies must determine if an integrated solution is cost effective and meets their operational requirements. CINCs, Services, and Agencies that operate PKI equipment will acquire appropriate training for their operators on the policy and proper use of the equipment. The Program Management Office, working with the Services, will develop the training material for any equipment that they develop.

5.6.1 Root CA(s)

NSA will manage and operate the DoD Root CA(s).

5.6.2 CA Servers and Central Directories

DISA will lead the integration and operations of the centralized certificate management and directory services. For CINC, Service, and Agency unique or tactical

applications, management and operation of those specific CA Servers falls to the CINC, Service, and Agency.

5.6.3 RAs and Local Directories

The CINCs, Services, and Agencies will initialize and operate the RAs and CINC, Service, and Agency local directories. Support will include registration, audit review, maintenance, and policy enforcement, operating a help desk, compromise recovery, re-key, and key recovery. The CINCs, Services, and Agencies will provide manning and workstations at the registration sites. The RA is envisioned to be a single person operation, but may require backups to provide continuous coverage in the event of illness or vacations.

5.6.4 Help Desk

The PMO will ensure that adequate Help Desk capabilities exist, consistent with the deployment of PKI products and services across the Department. It is expected that Help Desk capabilities will be decentralized.

5.7 Oversight

In February 1999, the DoD CIO approved the implementation plan for the Defense-wide Information Assurance Program (DIAP). The DIAP forms the Department's core organizing element for achieving a more comprehensive, coherent, and consistent IA program. It implements a process designed to provide for centralized planning, coordination, integration, and oversight of the Department's IA resources while retaining decentralized execution to realize continuous improvement in our IA posture. The DIAP's central coordination and oversight activities enable the Department to develop, validate, and prioritize DoD-wide IA requirements, determine the overall return of our IA investments, and objectively assess DoD's Defense-in-Depth efforts to protect information assets critical to the Department. This oversight will apply to all DoD PKI activities.

Appendix A.
Policy Management

The Policy Management process defines how DoD certificate policies will be approved and modified, and ensures that the policies are correctly implemented.

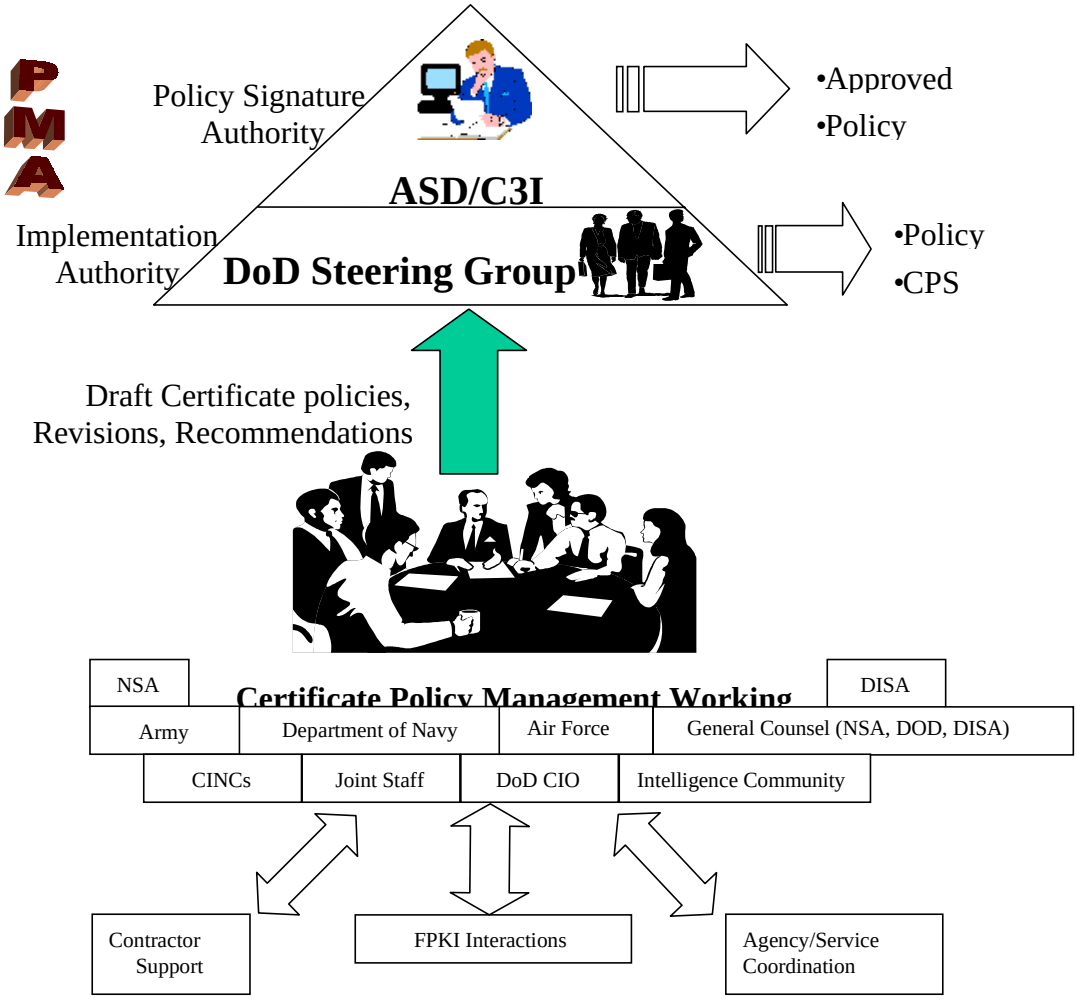

Figure 5. DoD Certificate Management Process

Policy Management Authority

OASD (C3I) is the Department of Defense public key certificate Policy Management Authority (PMA) for the DoD Certificate Policies (CPs). NSA has been designated as the Program Manager for the DoD PKI with DISA as the Deputy Program Manager.

Specifically, **OASD / C3I** will:

- Approve the DoD CPs; and
- Review, coordinate, and promulgate changes to the DoD CPs.

The DoD Steering Group will:

- Draft DoD CPs and any recommended changes to the CPs;
- Review Certification Practice Statements (CPSs) to ensure that they meet the requirements of DoD CPs;
- Review the CPs of external organizations with which the DoD PKI is considering cross-certification or otherwise certifying and make recommendations to the OASD(C3I) concerning which external security policies may be considered equivalent to DoD policies;
- Recommend to higher-echelon CAs that certain CA certificates be revoked, based on non-compliance with the CPs; and
- Issue formal statements to CAs to cease issuing certificates asserting DoD policies, should these CAs not comply with the DoD CPs.

The DoD PKI Program Manager will chair the DoD Steering Group. The following organizations shall be represented: NSA, DISA, Services, JCS, and OASD(C3I).

Certificate Policy Management Working Group (CPMWG)

The DoD PMA will establish a Certificate Policy Management Working Group (CPMWG) that will be responsible for advising the PMA to ensure that the DoD Certificate Policies are appropriate to the needs of the Department, and evolve to meet new operational and technical developments.

Specifically, the CPMWG will:

- Evaluate suggested modifications to the policies from the DoD, Services and Agencies;
- Provide timely, responsive, DoD, Service and Agency coordination and buy-in to the DoD CP through a consensus-building process;
- Ensure legal review is obtained for CP and any modifications;

- Review the Certification Practice Statements (CPS) of DoD-operated CAs and commercial CAs that offer to provide services to the DoD. The CPMWG will analyze the CPS documents to ensure that the practices of CAs serving the DoD comply with the DoD CP, and provide the analysis to the DoD Policy Management Authority;

- Analyze Federal, allied, commercial and other certificate policies with respect to DoD certificate policies for purposes of establishing the suitability of the non-DoD policies for use within the DoD (for example, in cases where the technical mechanism of "policy mapping" is being considered);

- Ensure that DoD certificate policies evolve to remain consistent with appropriate Federal, commercial, allied and international standards and practices. In particular, the DoD CPMWG will establish a liaison with the Federal PKI Legal and Policy Management Working Group;

Review the results of CA audits to determine if the CAs are adequately meeting the requirements of approved CPS documents. Make recommendations to the CAs and to the PMA regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates;

- Offer recommendations to PMA, DoD Program and Project Managers, and DoD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the various DoD certificate policies for specific applications; and

- Otherwise respond to the direction of the PMA to provide CP advice as required.

The DoD PKI Program Management Office will chair the CPMWG. The following organizations shall be represented on the CPMWG: NSA, DISA, the Intelligence Community, General Counsel, CINCs, Services, and Agencies, Office of the Joint Staff, Office of the DoD Chief Information Officer and other organizations as the PMA may direct.

Each organization may optionally provide operational, legal and technical representatives to the CPMWG as requested by the PMA or the CPMWG. Each member of the CPMWG (*except for the Legal Counsel*) represents all of the interests of their agency or department, and is responsible for coordinating a unified agency/department position on issues being considered by the CPMWG. CPMWG members must have the authority to speak on behalf of their agency or department.

The CPMWG will be expected to rely on the support of working-level personnel within the agencies represented on the CPMWG. Contractor support provided by the organizations represented on the CPMWG may also be used for such tasks as evaluating CPSs against the requirements of CPs, and evaluating policies of potential cross-certification partners. The CPMWG will meet on an as-needed basis. CPMWG recommendations will be by consensus. If consensus cannot be achieved, then the CPMWG will prepare a position paper and/or briefing for the PMA describing the issues involved, and the various points of view, and the PMA will make the final decision.

Appendix B.
DoD PKI Requests

This appendix identifies the process for requesting pilot program use of the DoD PKI.

Requests to use the DoD PKI

Until the DoD Class 3, 4 and Target PKIs are available, any requests for applications wishing to utilize the DoD medium assurance PKI pilot should be forwarded to the DoD PKI PMO. The DoD PKI PMO in coordination with OASD(C3I) and the Joint Staff will review/approve requests based upon cost and risk management factors.

CINCs, Services, and Agencies wishing to use the medium assurance PKI need to prepare and coordinate a risk assessment with the DoD PKI PMO prior to initiating the pilot. The risk assessment will describe what services are required from the infrastructure, as well as the sensitivity of the information to be protected.

Requests to Use Interim ECAs

Under the auspices of the DoD PKI PMO, a limited number of ECA pilots to provide interoperable Class 3 certificates to DoD contractors and other commercial entities will be initiated. These ECA pilots will be based on a variety of COTS PKI technologies and service providers. These ECA pilots will be used to derive the experience and cost benefit analysis data necessary to ensure optimum design of the DoD PKI. CINCs, Services, and Agencies wishing to use the IECAs need to prepare a request and forward it to the DoD PKI PMO for review and approval.

Appendix C.
Definitions

Assurance Levels: The level of assurance of a public key certificate is the degree of confidence in the binding of the identity to the public keys and privileges. Personnel, physical, procedural and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. DoD has defined 4 assurance levels in the US DoD X.509 Certificate Policy document (Reference A) . Per DoD PKI policy, t he DoD will use the following 3 classes:

Class 3: (Formerly Medium) This level is intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that require identification of an entity as a legal person, rather than merely a member of an organization. This assurance level requires that the end user register in person and their cryptography can be software based.

Guidance:

- Digital signature services for mission critical and national security information on an encrypted network;
- Key exchange for the protection of communities of interest (COIs) and low valued compartmented information on an encrypted network;
- Non-repudiation for medium value financial or electronic commerce applications such as payroll, some contracting, vehicle purchases, etc.

Class 4: (Formerly High) This level is intended for applications handling medium to high value information in any environment. These applications typically require identification of an entity as a legal person, rather than merely a member of an organization and a cryptographic hardware token for protection of the private key material. This level requires a hardware token for protection of private key material, and that the end user register in person.

Guidance

- Digital signature services for unclassified mission critical or national security information in an unencrypted network;
- Key exchange for confidentiality of high valued compartmented information on encrypted networks, and COIs or classified data over an unencrypted network on a case by case basis (e.g., FORTEZZA For Classified (FFC)) ;

- Protection of information crossing classification boundaries (e.g. sending information from NIPRNET to SIPRNET);

- Non-repudiation for large financial or electronic commerce applications.

Class 5: This level is intended for applications handling high value information in a high-risk environment. This assurance level requires National Security Agency (NSA)-approved Type I cryptography.

Guidance

- Key exchange for confidentiality of classified information over an unprotected network such as NIPRNET.

- Digital Signature services for authentication of subscriber identity and credentials in support of providing access to classified information over an unprotected network such as NIPRNET when used with appropriate encryption.

- Digital Signature services for authentication of key material in support of providing confidentiality services for classified information over an unprotected network such as NIPRNET.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Certificate: A computer-generated record that ties the user's identification with the user's public key in a trusted bond. The certificate contains the following (*at a minimum*): a version number, a serial number, identity of the issuing Certification Authority and the user, the user's public key, and validity dates.

Certificate Revocation List (CRL): A computer-generated record that identifies certificates that have been revoked prior to their expiration dates. It is periodically issued by each certification authority and posted to the directory.

Certification Authority (CA): An entity authorized to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate (e.g. control over the enrollment process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates and re-key). Additionally the CA is responsible for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in managing and issuing certificates in relation to a specific Certificate Policy.

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Data Recovery: The mechanisms and processes that allow authorized parties to recover the plaintext data when the decryption key has been lost or is otherwise unavailable.
Digital Signature: A transformation of a message using an asymmetric cryptographic system and a hash function such that a person having the initial message and the signer's public key can accurately determine if the transformation was created using the corresponding signer's private key. In addition, it can be determined if the initial message has been altered since the transformation was made.

Directory: The directory is a repository or database of certificates, CRLs, and other information available online to users.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (*one-way encryption*) or cannot be obtained without using the inverse decryption process.

Format Sensitive Information: The aggregation of information contained in a system is classified; therefore, the system must be able to handle information of that classification.

Integrity (Data Integrity): Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Key Exchange / Key agreement: A common cryptographic technique used to securely pass to each participant the encryption key(s) for a secure communications session.

Key Management Infrastructure (KMI): The framework and services that provide the generation, production, distribution, control, tracking and destruction for all cryptographic key material, symmetric keys as well as public keys and public key certificates.

Key Recovery: The mechanisms and processes that allow authorized parties to retrieve the cryptographic key used for data confidentiality when the original key lost or is otherwise unavailable.

Local Registration Authority (LRA): *See Registration Authority*.

Mission Category: Applicable to information systems, the category reflects the importance of information handled by the information system relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. DoD has three categories:

Mission Critical: Systems handling information determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms

of content and timeliness. It must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). Note: Mission critical systems include the following types of systems:

Category 1: Defined by the Clinger/Cohen Act as National Security Systems (NSS) (Intelligence Activities; Cryptologic Activities related to National Security; Command and Control of military forces, integral to a weapon or weapons system; systems critical to direct fulfillment of military or intelligence missions).

Category 2: In direct support of those systems identified by the CINCs which, if not functional, would preclude the CINC from conducting missions across the full spectrum of operations, including:

- Readiness (to include personnel management critical to readiness)
- Transportation
- Sustainment
- Modernization
- Surveillance/Reconnaissance
- Financial
- Security
- Safety
- Health
- Information Warfare
- Information Security
- Contractual

Category 3: Required to perform Department-level and Component-level core functions

Mission Support: Systems handling information that is important to the support of deployed and contingency forces. It must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified, but is more likely to be sensitive or unclassified).

Administrative: Systems handling information that is necessary for the conduct of the day-to-day business, but does not materially affect support to deployed forces or the readiness of contingency forces in the short term (may be classified, but is more likely to be sensitive or unclassified).

Non-Repudiation: Strong and substantial evidence of the identity of the signer, time, and context of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

Organizational Registration Authority (ORA): *See Registration Authority.*

Private Key: The part of a key pair to be safeguarded by the owner. A private key can be either a signature or key exchange key. Private signature keys are used to sign. Private key exchange keys are used with another party's public key to establish a shared key. It is computationally infeasible to determine a private key given the associated public key.

Public Key: The part of a key pair released to the public. A private key can be either a signature or key exchange key. The signer's public signature key is used to verify a digital signature.

Public Key Certificate: See Certificate.

Public Key Infrastructure (PKI): The framework and services that provide the generation, production, distribution, control, tracking and destruction of public key certificates.

Registration Authority (RA): The person who is responsible to the CA for local (*onsite*) identification of users' identity.

Root Certification Authority: The Root CA is a trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.

Token: A physical device (e.g. *floppy diskette, smart card, PC Card, etc.*) which is used to protect and transport the private keys of a user.

Appendix D. PKI Milestones

The following represent milestones to be met by the DoD PKI:

IMMEDIATELY

- All DoD organizations must deploy registration applications for supporting the Class 3 (formerly Medium Assurance) PKI and the Class 4 (FORTEZZA-based)PKI.

IMMEDIATELY – (Initial Operational Capability)

JUNE 2000 – (Full Operational Capability)

- ***Protection*** of Category 1 mission critical systems on unencrypted networks using Class 4 certificates and tokens.

IMMEDIATELY

- ***Protection*** of Category 2/3 mission critical systems operating on unencrypted networks must use Class 3 certificates

IMMEDIATELY – (Initial Operational Capability)

31 DECEMBER 2002 - (Full Operational Capability)

- ***Protection*** of Category 2/3 mission critical systems operating on unencrypted networks must use Class 4 certificates and tokens

JUNE 2000 - ***SERVER AUTHENTICATION***

OCTOBER 2001 - ***CLIENT IDENTIFICATION AND AUTHENTICATION***

- Private DoD web servers access control software for Class 3 certificates

OCTOBER 2001

- Email applications to facilitate digital signature processing of all individual messaging within DoD using Class 3 certificates

JANUARY 2002 - (Initial Operational Capability)

- ID card processing software, building/facility access software, and workstation access software applications shall begin implementation for Class 4 certificates

References

A. US DoD X.509 Certificate Policy (CP), October 1999.

B. Deputy Secretary of Defense, Department of Defense (DoD) Public Key Infrastructure (PKI), May 6, 1999, Washington, DC.

C. OASD(C3I), Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI), April 9, 1999, Washington, DC.

D. Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations, Federal Public Key Infrastructure (FPKI) Technical Working Group (TWG), 4 September 1998.

E. Public-Key Cryptography Standard (PKCS) #10: Certification Request Syntax Standard, Version 1.0, November 1, 1993.

F. RFC 2511, Internet X.509 Certificate Request Message Format, March 1999.

G. The Common Criteria for Information Technology Security Evaluation (CC), Version 2.1 / ISO IS 15408, 5 October 1999.

H. Information Assurance Technical Framework, Release 2.0.1, September 1999.

I. Public Key Infrastructure Implementation Plan for the Department of Defense, Version 2.0, 29 October 1999

J. Public Key Infrastructure – A Technology Forecast, NSA Office of INFOSEC Research and Technology August 1999

K. Federal Information Processing Standards (FIPS) Publication 140-1 1994 January 11.

Abbreviations and Acronyms

ASD (C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
CA	Certification Authority
CINC	Commander in Chief
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CPMWG	Certificate Policy Management Working Group
CRL	Certificate Revocation List
C/S/A	CINCs, Services and Agencies
CY	Calendar Year
DIAP	Defense-wide Information Assurance Program
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DMS	Defense Message System
DNS	Domain Name Server
DoD	Department of Defense
ECA	External Certification Authority
EKMS	Electronic Key Management System
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FY	Fiscal Year
GOTS	Government Off-The-Shelf
I&A	Identification and Authentication
IA	Information Assurance
IT	Information Technology

KMI	Key Management Infrastructure
LAN	Local Area Network
NIPRNET	Non-classified Internet Protocol Router Network
NIAP	National Information Assurance Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PC	Personal Computer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PMI	Privilege Management Infrastructure
RA	Registration Authority
S	Secret
S/A	Service or Agency
SIPRNET	Secret Internet Protocol Router Network
TLS	Transport Layer Security
TS	Top Secret
U	Unclassified
WAN	Wide Area Network